

This Page Is Inserted by IFW Operations  
and is not a part of the Official Record

## **BEST AVAILABLE IMAGES**

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images may include (but are not limited to):

- BLACK BORDERS
- TEXT CUT OFF AT TOP, BOTTOM OR SIDES
- FADED TEXT
- ILLEGIBLE TEXT
- SKEWED/SLANTED IMAGES
- COLORED PHOTOS
- BLACK OR VERY BLACK AND WHITE DARK PHOTOS
- GRAY SCALE DOCUMENTS

**IMAGES ARE BEST AVAILABLE COPY.**

As rescanning documents *will not* correct images,  
please do not report the images to the  
Image Problem Mailbox.

IN THE CLAIMS:

Amended claims follow:

1. (Currently Amended) A system for analyzing a network, scanning the network, and detecting intrusions in the network, comprising:
  - (a) a plurality of agents coupled to a plurality of computers interconnected via a network, each agent adapted to collect information;
  - (b) a plurality of host controllers coupled to the agents for collecting the information from the agents, scanning the information, and detecting intrusions in the network; and
  - (c) a plurality of zone controllers coupled to the host controllers for analyzing an output of the host controllers, and executing security actions in response thereto; wherein a report is generated including a plurality of objects in a tree representation;  
wherein intrusion detection services are provided based on the information;  
wherein a Simple Network Management Protocol (SNMP) trap capability is utilized.
2. (Original) The system as recited in claim 1, wherein the host controllers are further capable of cybercop services.
3. (Original) The system as recited in claim 1, wherein the zone controllers are further capable of integrated reporting.
4. (Original) The system as recited in claim 1, wherein the host controllers and the zone controllers operate based on business rules.
5. (Original) The system as recited in claim 1, wherein the business rules are user-configurable.

6. (Currently Amended) A method for analyzing a network, scanning the network, and detecting intrusions in the network, comprising:
- (a) collecting information relating to a plurality of computers utilizing a plurality of agents coupled to the computers via a network;
  - (b) collecting the information from the agents utilizing a plurality of host controllers coupled to the agents;
  - (c) scanning the information utilizing the host controllers;
  - (d) detecting intrusions in the network utilizing the host controllers;
  - (e) collecting the information from the host controllers utilizing a plurality of zone controllers coupled to the host controllers;
  - (f) analyzing output of (b)-(d) utilizing the zone controllers; and
  - (g) executing security actions based on the analysis utilizing the zone controllers; wherein a report is generated including a plurality of objects in a tree representation;  
wherein intrusion detection services are provided based on the information;  
wherein a Simple Network Management Protocol (SNMP) trap capability is utilized.
7. (Original) The method as recited in claim 6, wherein the host controllers are further capable of cybercop services.
8. (Original) The method as recited in claim 6, wherein the zone controllers are further capable of integrated reporting.
9. (Original) The method as recited in claim 6, wherein the host controllers and the zone controllers operate based on business rules.
10. (Original) The method as recited in claim 6, wherein the business rules are user-configurable.

11. (Currently Amended) A computer program product for analyzing a network, scanning the network and detecting intrusions in the network, comprising:
- (a) computer code for collecting information relating to a plurality of computers utilizing a plurality of agents coupled to the computers via a network;
  - (b) computer code for collecting the information from the agents utilizing a plurality of host controllers coupled to the agents;
  - (c) computer code for scanning the information utilizing the host controllers;
  - (d) computer code for detecting intrusions in the network utilizing the host controllers;
  - (e) computer code for collecting the information from the host controllers utilizing a plurality of zone controllers coupled to the host controllers;
  - (f) computer code for analyzing output of (b)-(d) utilizing the zone controllers; and
  - (g) computer code for executing security actions based on the analysis utilizing the zone controllers;
- wherein a report is generated including a plurality of objects in a tree representation;
- wherein intrusion detection services are provided based on the information;
- wherein a Simple Network Management Protocol (SNMP) trap capability is utilized.
12. (Original) The computer program product as recited in claim 11, wherein the host controllers are further capable of cybercop services.
13. (Original) The computer program product as recited in claim 11, wherein the zone controllers are further capable of integrated reporting.
14. (Original) The computer program product as recited in claim 11, wherein the host controllers and the zone controllers operate based on business rules.

15. (Original) The computer program product as recited in claim 14, wherein the business rules are user-configurable.
16. (Currently Amended) A system for analyzing a network, scanning the network and detecting intrusions in the network, comprising:
- (a) agent means adapted to collect information;
  - (b) host controller means for collecting the information from the agent means, scanning the information, and detecting intrusions in the network; and
  - (c) zone controller means for analyzing an output of the host controller means, and executing security actions in response thereto;
- wherein a report is generated including a plurality of objects in a tree representation;
- wherein intrusion detection services are provided based on the information;
- wherein a Simple Network Management Protocol (SNMP) trap capability is utilized.
17. (Original) The system as recited in claim 16, wherein the host controller means is further capable of cybercop services.
18. (Original) The system as recited in claim 16, wherein the zone controller means is further capable of integrated reporting.
19. (Original) The system as recited in claim 16, wherein the host controller means and the zone controller means operate based on business rules.
20. (Original) The system as recited in claim 19, wherein the business rules are user-configurable.

21. (Currently Amended) A system for analyzing a network, scanning the network, and detecting intrusions in the network, comprising:
- (a) a plurality of agents coupled to a plurality of computers interconnected via a network, each agent adapted to collect information;
  - (b) a plurality of host controllers coupled to the agents for collecting the information from the agents;
  - (c) means for scanning the information;
  - (d) means for detecting intrusions in the network;
  - (e) a plurality of zone controllers coupled to the host controllers for analyzing an output of the host controllers; and
  - (f) means for executing security actions in response to at least one of the scanning, the detecting, and the analyzing;
- wherein a report is generated including a plurality of objects in a tree representation;
- wherein intrusion detection services are provided based on the information;
- wherein a Simple Network Management Protocol (SNMP) trap capability is utilized.

22. (Currently Amended) A method for providing business rule-based network services utilizing a network, comprising:
- (a) collecting information relating to a plurality of computers utilizing a plurality of agents coupled to the computers via a network;
  - (b) collecting the information from the agents utilizing a plurality of controllers coupled to the agents;
  - (c) identifying a plurality of business rules; and
  - (d) providing services utilizing the information based on the business rules;
- wherein a report is generated including a plurality of objects in a tree representation;
- wherein intrusion detection services are provided based on the information;

wherein a Simple Network Management Protocol (SNMP) trap capability is utilized.

23. (Original) The method as recited in claim 22, wherein the services include analysis services, intrusion detection services, anti-virus services, and security services.
24. (Original) The method as recited in claim 22, wherein the services include at least one of analysis services, intrusion detection services, anti-virus services, and security services.
25. (Currently Amended) A system for analyzing a network and detecting intrusions in the network, comprising:
  - a plurality of information collectors coupled to a plurality of computers interconnected via a network, each information collector adapted to collect information;
  - at least one information collector manager coupled to the information collectors for collecting the information from the information collectors, and detecting intrusions in the network; and
  - a user interface for analyzing an output of the information collector manager;

wherein a report is generated including a plurality of objects in a tree representation;

wherein intrusion detection services are provided based on the information;

wherein a Simple Network Management Protocol (SNMP) trap capability is utilized.
26. (Original) The system as recited in claim 25, wherein the information relates to wireless network traffic.

27. (Currently Amended) A method for analyzing a network and detecting intrusions in the network, comprising:  
collecting information relating to a plurality of computers utilizing a plurality of information collectors coupled to the computers via a network;  
collecting the information from the information collectors utilizing at least one information collector manager coupled to the information collectors; and  
detecting intrusions in the network based on an analysis utilizing the information;  
wherein security actions are capable of being carried out based on the analysis;  
wherein a report is generated including a plurality of objects in a tree representation;  
wherein intrusion detection services are provided based on the information;  
wherein a Simple Network Management Protocol (SNMP) trap capability is utilized.
28. (Original) The method as recited in claim 27, wherein the information relates to wireless network traffic.
29. (New) The system as recited in claim 1, wherein enterprise latency mapping is performed.
30. (New) The system as recited in claim 29, wherein at least one of the zone controllers chooses a port number associated with an application.
31. (New) The system as recited in claim 30, wherein the at least one zone controller pushes a configuration request to a plurality of the host controllers in an associated zone.



32. (New) The system as recited in claim 31, wherein the host controllers push the configuration request to the agents.
33. (New) The system as recited in claim 32, wherein the agents monitor a port associated with the port number.
34. (New) The system as recited in claim 33, wherein monitor data is sent from the agents to the host controllers.
35. (New) The system as recited in claim 34, wherein the monitor data is buffered.
36. (New) The system as recited in claim 34, wherein the host controllers update the at least one zone controller with consolidated monitor data.
37. (New) The system as recited in claim 36, wherein differences in delay times are calculated to construct a picture of latency throughout an enterprise.